08-21-00

A

LERNER AND GREENBERG, P.A.

PATENT ATTORNEYS AND ATTORNEYS AT LAW

2445 Hollywood Boulevard
Hollywood, Florida 33020
Tel: (954) 925-1100
Fax: (954) 925-1101

Herbert L. Lerner (NY Bar)
Laurence A. Greenberg (FL Bar)

Werner H. Stemer (FL Bar), Senior Attorney

Ralph E. Locher (FL, IL, MO Bars)
Manfred Beck (US & German Pat. Agent)
Mark P. Weichselbaum (TN Bar)
Gregory L. Mayback (FL Bar)
Markus Nolff (FL Bar)
Otto S. Kauder (Reg. Pat. Agent)
Loren Donald Pearson (FL Bar)

www.patentusa.com
patents@patentusa.com

Mailing Address:
Post Office Box 2480
Hollywood, FL 33022-2480

New York Office
153 E 57th Street
Suite 15G
New York, NY 10022

"Express Mail" mailing label number EL608558180US
Date of Deposit August 18, 2000

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Docket No.: GR 98 P 1180

Michael Burns
MICHAEL BURNS

Date: August 18, 2000

Hon. Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Enclosed herewith are the necessary papers for filing the following application for Letters Patent:

Applicant : ERWIN HESS ET AL.

Title : METHOD AND DEVICE FOR CRYPTOGRAPHIC PROCESSING WITH THE AID OF AN ELLIPTIC CURVE ON A COMPUTER

4 sheets of formal drawings in triplicate.
A check in the amount of $ 690.00 covering the filing fee.

This application is being filed without a signed oath or declaration under the provisions of 37 CFR 1.53(d). Applicants await notification of the date by which the oath or declaration and the surcharge are due, pursuant to this rule.

The Patent and Trademark Office is hereby given authority to charge Deposit Account No. 12-1099 of Lerner and Greenberg, P.A. for any fees due or deficiencies of payments made for any purpose during the pendency of the above-identified application.

Respectfully submitted,

W. Stemer

For Applicants

WERNER H. STEMER
REG. NO. 34,956

LAG:kc

GR 98 P 1180

METHOD AND DEVICE FOR CRYPTOGRAPHIC PROCESSING WITH THE AID OF AN ELLIPTIC CURVE ON A COMPUTER

Cross-Reference to Related Application:

This is a continuation of copending International Application PCT/DE99/00278, filed February 2, 1999, which designated the United States.

Background of the Invention:

Field of the Invention:

The invention relates to a method and a device for cryptographic processing with the aid of an elliptic curve on a computer.

A finite body is called a finite field. Reference may be made to Lidl and Niederreiter: Introduction to Finite Fields and Their Applications, Cambridge University Press, Cambridge 1986, ISBN 0-521-30706-6, p. 15, 45, concerning the properties and definition of the finite field.

Increasingly growing demands are being placed on data security with the wide dissemination of computer networks and associated applications which are being developed over

electronic communication systems (communications networks). The aspect of data security takes account of, inter alia,

- the possibility of a failure of data transmission;
- the possibility of corrupted data;
- the authenticity of the data, that is to say the possibility of establishing, and the identification of a sender; and
- the protection of the secrecy of the data.

A "key" is understood as data which are used in cryptographic processing. It is known from public-key methods to use a secret and a public key. Reference is had, in this context, to Christoph Ruland: Informationssicherheit in Datennetzen [Information Security in Data Networks], DATACOM-Verlag, Bergheim 1993, ISBN 3-892238-081-3, p. 73-85.

An "attacker" is defined as an unauthorized person who aims at obtaining the key or breaking the key.

Particularly in a computer network, but increasingly also in portable media, for example a mobile telephone, a chip card or smart card, it is to be ensured that a stored key also cannot be accessed when an attacker takes over the computer, the mobile telephone or the chip card.

In order to ensure adequate security of cryptographic methods, keys, in particular in the case of asymmetric methods, are respectively determined with lengths of several 100 bits. A memory area of a computer or portable medium is mostly of meager dimension. A length of a key of several 100 bits stored in such a memory area reduces the free memory space on the computer or the medium, such that only a few such keys can be stored at the same time.

An elliptic curve and its use in cryptographic processing are known in the literature, for example: Neal Koblitz: A Course in Number Theory and Cryptography, Springer Verlag, New York, 1987, ISBN 0-387-96576-9, p. 150-79; and Alfred J. Menezes: Elliptic Curve Public Key Cryptosystems, Luwer Academic Publishers, Massachusetts 1993, ISBN 0-7923-9368-6, p. 83-116.

Summary of the Invention:

The object of the invention is to provide a method and device for cryptographic processing with an elliptic curve on a computer which overcomes the above-noted deficiencies and disadvantages of the prior art devices and methods of this kind, and which requires less memory space.

With the above and other objects in view there is provided, in accordance with the invention, a method of cryptographic processing on a computer, which comprises the steps of:

prescribing an elliptic curve in a first form, the elliptic curve having a plurality of first parameters;

transforming the elliptic curve into a second form

$$y^2 = x^3 + c^4ax + c^6b$$

by determining a plurality of second parameters, wherein at least one of the second parameters is shortened in length by comparison with the first parameter;

wherein x, y are variables;

a, b are the first parameters; and

c is a constant;

wherein at least the parameter a is shortened by selecting the constant c such that

$$c^4a \bmod p$$

is determined to be significantly shorter than a length of the parameter b and the length of the prescribed variable p; and

determining the elliptic curve in the second form for cryptographic processing.

A method for cryptographic processing with the aid of at least one elliptic curve on a computer is specified, in the case of which the elliptic curve is prescribed in a first form, several first parameters determining the elliptic curve in the first form. The elliptic curve is transformed into a second form by determining several second parameters, at least one of the second parameters being shortened in length by comparison with one of the first parameters. The elliptic curve after the transformation, that is to say in the second form, is used for the cryptographic processing.

The significant shortening of one of the first parameters yields a saving of a memory area which is to be provided for this parameter. Since the memory area, for example on a chip card, is of tight dimension, free memory space is achieved for each shortened parameter by means of the saving of several 100 bits, for example for storing a further secret key. The security of the cryptographic method is ensured nevertheless by the shortening of the respective parameter.

In the case of the use of an elliptic curve in a cryptographic method, the outlay for an attacker to determine the key rises exponentially with its length.

In accordance with an added feature of the invention, the first form of the elliptic curve is defined by

$$y^2 = x^3 + ax + b \text{ over } GF(p) \qquad (1)$$

wherein

GF(p) denotes a finite field with p elements; and

x,y,a,b denoting elements of the body GF(p).

Designation "mod p" as used in this text denotes a special case for the finite field, specifically the natural numbers smaller than p. The term "mod" stands for MODULO, and comprises an integral division with remainder.

The second form, as noted above, of the elliptic curve is determined by

$$y^2 = x^3 + c^4ax + c^6b \text{ over } GF(p) \qquad (2)$$

where c is a constant.

In order to save memory space, Equation (1) is transformed into Equation (2), and a variable characterizing the elliptic curve in accordance with Equation (2) is shortened.

The invention is preferably integrated in cryptographic encoding, cryptographic decoding, key allocation, encoding in

a digital signature, verification of the digital signature, and in asymmetrical authentication, that is:

- Encoding and decoding:
  Data are encoded by a sender - by means of symmetrical or asymmetrical methods - and decoded at the other end at a receiver.

- Key allocation by a certification authority:
  A trustworthy institution (certification authority) allocates the key, it being necessary to ensure that the key comes from this certification authority.

- Digital signature and verification of the digital signature:
  An electronic document is signed, and the signature is added to the document. It can be established at the receiver with the aid of the signature whether the desired sender really has signed.

- Asymmetric authentication:
  A user can verify his identity with the aid of an asymmetrical method. This is preferably done by coding using a corresponding private key. Using the associated public key of this user, anyone can establish that the code really does come from this user.

- Shortening of keys:

  A variant of the cryptographic processing comprises shortening a key, which key can preferably be used for further procedure in cryptography.

With the above and other objects in view there is also provided, in accordance with the invention, a device for cryptographic processing with a processor unit programmed to:

prescribe an elliptic curve in a first form, with a plurality of first parameters determining the elliptic curve;

transform the elliptic curve into a second form

$$y^2 = x^3 + c^4ax + c^6b$$

by determining a plurality of second parameters, at least one of the second parameters being shortened in length by comparison with the first parameter;

wherein x,y are variables;

a,b are the first parameters; and

c is a constant;

shorten the at least the parameter a by selecting the constant c such that

$$c^4a \bmod p$$

can be determined to be much shorter than the length of the parameter b and the length of the prescribed variable p; and

determine the elliptic curve in the second form for the purpose of cryptographic processing.

In accordance with an additional feature of the invention, the device is embodied as a chip card (smart card) with a memory area, the memory area being adapted to store the parameters of the elliptic curve.

In accordance with a concomitant feature of the invention, the chip card has a protected memory area adapted to store a secret key.

In other words, the device has a processor unit which is set up in such a way that an elliptic curve is prescribed in a first form, several first parameters determining the elliptic curve, and that the elliptic curve is transformed into a second form by determining several second parameters, at least one of the second parameters being shortened in length by comparison with the first parameters. Finally, the elliptic curve is determined in the second form for the purpose of cryptographic processing.

This device can be a chip card which has a protected and a non-protected memory area. Keys, that is to say parameters which characterize the elliptic curve, can be stored both in the protected memory area and in the non-protected one.

This device is particularly suited to carrying out the method according to the invention or one of its developments explained above.

Finally, there is also defined a computer-readable medium which carries the computer-executable instructions for carrying out the above-outlined method.

Other features which are considered as characteristic for the invention are set forth in the appended claims.

Although the invention is illustrated and described herein as embodied in a method and device for cryptographic processing with the aid of an elliptic curve on a computer, it is nevertheless not intended to be limited to the details shown, since various modifications and structural changes may be made therein without departing from the spirit of the invention and within the scope and range of equivalents of the claims.

The construction and method of operation of the invention, however, together with additional objects and advantages

thereof will be best understood from the following description of specific embodiments when read in connection with the accompanying drawings.

Brief Description of the Drawings:

Fig. 1 is a flowchart illustrating a method for cryptographic processing by means of an elliptic curve according to the invention, wherein at least one parameter of the elliptic curve is shortened, which leads to a space savings of a part of the memory area required for the parameters of the elliptic curve;

Fig. 2 is a flowchart showing a selection of options for the prime number p such that the parameter a of the elliptic curve is shortened;

Fig. 3 is a flowchart showing a method for determining an elliptic curve and subsequent transformation into the second form;

Fig. 4 is a diagrammatic view of a system for cryptographic processing; and

Fig. 5 is a schematic view of a processor unit.

Description of the Preferred Embodiments:

Referring now to the figures of the drawing in detail and first, particularly, to Fig. 1 thereof, there is illustrated a method for processing by means of an elliptic curve. The elliptic curve is present in a first form in block 101. In block 102, the curve is transformed from the first form into a second form. Then, a parameter of the second form is shortened in block 103, and the second form is stored for the purpose of cryptographic processing in block 104. These steps will be discussed below, with options for shortening being taken by way of example.

The elliptic curve is first given in a first form:

$$y^2 = x^3 + ax + b \text{ over } GF(p) \qquad (3)$$

The length of the parameter a is reduced in a first step. The parameter p is, in particular, a prime number greater than 3, and GF(p) represents a finite field (Galois field) with p elements.

The elliptic curve

$$y^2 = x^3 + ax + b \text{ over } GF(p) \qquad (4)$$

can be recast by a transformation into a birational isomorphic elliptic curve (elliptic curve in second form, see block 102)

$$y^2 = x^3 + c^4ax + c^6b \text{ over } GF(p) \qquad (5).$$

The coefficient

c^4a or (6)

$-c^4a$ (7)

can be shortened by suitable selection of the constant c (see block 103) with the advantage that the memory space required for storing this coefficient can be small by comparison with the memory space for the parameter a.

The numbers

c^4a (or $-c^4a$) and c^2

are determined below in accordance with Equation (5).

<u>Determining the number "c^4a"</u>

The following cases are preferably distinguished in order to determine the number c^4a (or $-c^4a$)

a) p 3 mod 4

It holds in these bodies that:

- all squares are also fourth powers; and
- '-1' is not a square.

Now let $p = 4k + 3$ and s be a fourth power which generates the multiplicative subgroup of the fourth powers (or the squares) in GF(p).

By definition

$V = \{1, s, s^2, s^3, \ldots, s^{2k}\}$ is the set of the fourth powers in GF(p) and

$NQ = \{-1, -s, -s^2, -s^3, \ldots, -s^{2k}\}$ is the set of the non-squares in GF(p)

1. For each element $a = s^t$ from V there exists an element $c^4 = s^{2k+1-t}$ from V with $c^4 a = s^{2k+1} = 1$ in GF(p).

2. For each element $a = -s^t$ from V there exists an element $c^4 = s^{2k+1-t}$ from V with $c^4 a = -s^{2k+1} = -1$ in GF(p).

In this case s, t and k denote body elements from GF(p).

For p 3 mod 4, the parameter a can be converted by suitable selection of the constant c into the number $c^4 a = 1$ in GF(p) or $c^4 a = -1$ in GF(p).

b) p 1 mod 4

It holds in such a body that:

- (p-1)/4 elements of the multiplicative group of the body are fourth powers;
- (p-1)/4 elements of the multiplicative group of the body are squares, but not fourth powers;
- (p-1)/2 elements of the multiplicative group of the body are non-squares;
- '-1' is not a non-square.

b1) p 5 mod 8

It holds in addition in such a body that:

- '-1' is a square but not a fourth power; and
- '+2', '-2' are non-squares.

Now let $p = 8k + 5$ and s be a fourth power which generates the multiplicative subgroup of the fourth power in GF(p).

By definition

$V = \{1, s, s^2, s^3, \dots, s^{2k}\}$	is the set of the fourth powers in GF(p) and
$Q = \{-1, -s, -s^2, -s^3, \dots, -s^{2k}\}$	is the set of squares which are not fourth powers in GF(p), and
$NQ = \{2, 2s, 2s^2, 2s^3, \dots, 2s^{2k}, -2, -2s, -2s^2, -2s^3, \dots, -2s^{2k}\}$	is the set of non-squares in GF(p).
1. For each element there exists an element with	$a = s^t$ from V $c^4 = s^{2k+1-t}$ from V $c^4a = s^{2k+1} = 1$ in GF(p).
2. For each element there exists an element with	$a = -s^t$ from Q $c^4 = s^{2k+1-t}$ from V $c^4a = -s^{2k+1} = -1$ in GF(p).
3. For each element there exists an element with	$a = s^t$ from NQ $c^4 = s^{2k+1-t}$ from V $c^4a = 2s^{2k+1} = 2$ in GF(p).
4. For each element there exists an element with	$a = -2s^t$ from NQ $c^4 = s^{2k+1-t}$ from V $c^4a = -2s^{2k+1} = -2$ in GF(p).

For p 5 mod 8, the parameter a can be converted into the number

$$c^4a = 1 \text{ or } -1 \text{ or } 2 \text{ or } -2 \text{ in } GF(p)$$

by suitable selection of the constant c.

b2) p 1 mod 8

The number c^4a can be determined according to the following scheme:

For r=1,-1,2,-2,3,-3,4,-4,…

- form $z = ra^{-1} \bmod p$;
- calculate $u = z^{(p-1)/4} \bmod p$;
- terminate if u=1; and
- store $z = c^4$ and $r = c^4a$.

Determining the number "c^2 in GF(p)"

In order to determine the number c^2 mod.p, it is first established in the appropriate body GF(p) whether a is a fourth power, a square but not a fourth power, or a non-square.

a) $p = 4k + 3$

The term $u = a^{(p-1)/2}$ in GF(p) is calculated in these bodies.

- If u=1 in GF(p), a is a fourth power (or a square). In this case, $c^4 = a^{-1}$ in GF(p).
- If u=1 in GF(p), a is a non-square. In this case, $c^4 = -a^{-1}$ in GF(p).

b) $p = 8k + 5$

The term $u = a^{(p-1)/4}$ in GF(p) is calculated in these bodies.

- If u=1 in GF(p), a is a fourth power. In this case, $c^4 = a^{-1}$ in GF(p).
- If u=-1, a is a square but not a fourth power. In this case, $c^4 = -a^{-1}$ in GF(p).
- If u is neither 1 nor -1 in GF(p), a is a non-square in GF(p). In this case, $v = (2a)^{(p-1)/4}$ in GF(p) is calculated. If v=1 in GF(p), $c^4 = 2a^{-1}$ in GF(p), otherwise $c^4 = -2a^{-1}$ in GF(p).

c) $p = 8k + 1$

According to the scheme described in b2) above, $z = c^4$ in these bodies.

The two roots (c^2 and $-c^2$) of c^4 can be calculated in all three cases with an outlay of O(log p). For the case $p = 4k + 3$, only one of the two specified solutions is permissible, specifically that which is a square in GF(p). Both solutions are permissible in the other cases. Coefficient c^6b of the elliptic curve can thus be calculated.

Such prime numbers are to be preferred in practice because of the closed formulas for the cases $p = 4k + 3$ and $p = 8k + 5$.

Example 1:

Let the prime number $p = 11 \Rightarrow$ Case a: $p = 3 \bmod 4$

Number	Squares Q	Fourth powers V
1	1	1
2	4	5
3	9	4
4	5	3
5	3	9
6	3	9
7	5	3
8	9	4
9	4	5
10	1	1

Table 1: Squares and fourth powers mod 11

The set of the squares Q, the set of the fourth powers V and the set of the non-squares NQ are thereby yielded as:

$Q = V = (1,3,4,5,9)$;

$NQ = (2,6,7,8,10)$.

$\underline{a \in V = Q} \Rightarrow ac^4 = 1$

a=	c^4=
1	1
3	4
4	3
5	9
9	5

Table 2: Determination of c^4 for a given parameter a

$\underline{a \in NQ}$ $\Rightarrow$ $ac^4 = -1$

$a=$	$c^4=$
2	5
6	9
7	3
8	4
10	1

Table 3: Determination of c^4 for a given parameter a.

Table 2 shows various options for a value assignment of a and c^4 which always yield 1 in the combination ac^4, and Table 3 shows various options for a value assignment of a and c^4 which always yield −1 in the combination ac^4. This holds in GF(11).

<u>Example 2</u>:

Let the prime number $p = 13$ $\Rightarrow$ Case b1): $p = 1 \bmod 4$ and, at the same time, $p = 5 \bmod 8$

Number	Squares Q	Fourth powers V
1	1	1
2	4	3
3	9	3
4	3	9
5	12	1
6	10	9
7	10	9
8	12	1
9	3	9
10	9	3
11	4	3
12	1	1

Table 4: Squares and fourth powers mod 13

The set of the squares Q (which are not fourth powers), the set of the fourth powers V and the set of the non-squares NQ are thereby yielded as:

Q = (4,10,12);

V = (1,3,9);

NQ = (2,5,6,7,8,11).

<u>$a \in V$</u> $\Rightarrow$ $c^4 \in V$

a=	c^4=
1	1
3	9
9	3

Table 5: Determination of c^4 for a given parameter a

$\Rightarrow ac^4 \quad 1 \bmod 13$

<u>$a \in Q$</u>

a=	c^4 =	ac^4 =
4	3	12 = -1 mod 13
10	9	90 = -1 mod 13
12	1	12 = -1 mod 13

Table 6: Determination of c^4 for a given parameter a

$\Rightarrow ac^4 = -1 \bmod 13$

<u>$a \in NQ$</u>

NQ = (2,5,6,7,8,11), with

2*V = (1,5,6) and

2*Q = (7,8,11)

<u>Case a:</u> $a \in NQ$ and $a \in (2 * V)$

a=	c^4 =	ac^4 =
2	1	2 = 2 mod 13
5	3	15 = 2 mod 13
6	9	54 = 2 mod 13

Table 7: Determination of c^4 for a given parameter a

$\Rightarrow ac^4 = 2 \bmod 13$

Case b: $a \in NQ$ and $a \in (2 * Q)$

$a=$	$c^4 =$	$ac^4 =$
7	9	$63 = -2 \bmod 13$
8	3	$24 = -2 \bmod 13$
11	1	$11 = -2 \bmod 13$

Table 8: Determination of c^4 for a given parameter a

$\Rightarrow ac^4 = -2 \bmod 13$

The elliptic curve obtained in the manner described in the second form (see block 103) is used for the purpose of cryptographic processing.

Referring now to Fig. 2, there is shown a range of options for the selection of the prime number p for the purpose of shortening the parameter a (see block 201), as described above. The option 202 determines p in such a way that p = 3 mod 4 holds. In this case, the parameter a can be shortened with the aid of the mode of procedure described above. The same holds for p = 1 mod 4 (Case 203), two cases p = 5 mod 8 (Case 204) and p = 1 mod 8 (Case 205) being advanced separately to distinguish them. The closed formulations for determining a shortened parameter a are likewise set forth above. Fig. 2 shows explicitly a selection of options without attempting to claim a comprehensive selection.

An elliptic curve with the parameters a, b, p and a number of points ZP is determined in accordance with Equation (1) in a first step 301 in Fig. 3. The elliptic curve is transformed in a step 302 (compare Equation (2)). After the transformation, the elliptic curve comprises the parameters a', b', p and ZP. a' and b' indicate that the parameters a and b have been changed, one parameter, preferably the parameter a' being short by comparison with the parameter a, such that memory space is saved by storing the parameter a' instead of the parameter a as a characteristic of the elliptic curve.

Referring now to Fig. 4, there is shown, in diagrammatic form, a system for cryptographic processing. A portable medium 401, preferably a chip card, comprises an (insecure) memory area MEM 403 and a protected (secure) memory area SEC 402. Data are exchanged between the medium 401 and a computer network 406 by a channel 405 with the aid of an interface IFC 404. The computer network 406 comprises several computers, which are interconnected and intercommunicate. Data for operating the portable medium 401 are preferably available in a distributed fashion in the computer network RN 406.

The protected memory area 402 is designed to be unreadable. The data of the protected memory area 402 are used with the aid of an arithmetic-logic unit which is accommodated on the portable medium 401 or in the computer network 406. A

comparative operation can therefore specify as result whether a comparison of an input with a key in the protected memory area 402 was successful or not.

The parameters of the elliptic curve are stored in the protected memory area 402 or in the unprotected memory area 403. In particular, a secret or private key is stored in the protected memory area, and a public key is stored in the insecure memory area.

An arithmetic-logic unit 501 is illustrated in Fig. 5. The arithmetic-logic unit 501 comprises a processor CPU 502, a memory 503 and an input/output interface 504 which is used in different ways via an interface 505 led out of the arithmetic-logic unit 501: an output on a monitor 507 is visualized via a graphics interface, and/or output on a printer 508. An input is performed via a mouse 509 or a keyboard 510. The arithmetic-logic unit 501 also has a bus 506 which ensures the connection between the memory 503, processor 502 and input/output interface 504. It is also possible to connect additional components with the bus 506: additional memory, fixed disk, etc..

The term "computer-readable medium," as used in this text, includes any kind of computer memory such as floppy disks,

removable disks, hard disks, CD-ROMs, flash ROMs, non-volatile ROMs, and RAM.

We claim:

1. A method of cryptographic processing on a computer, which comprises the steps of:

prescribing an elliptic curve in a first form, the elliptic curve having a plurality of first parameters;

transforming the elliptic curve into a second form

$$y^2 = x^3 + c^4ax + c^6b$$

by determining a plurality of second parameters, wherein at least one of the second parameters is shortened in length by comparison with the first parameter;

wherein x,y are variables;

a,b are the first parameters; and

c is a constant;

wherein at least the parameter a is shortened by selecting the constant c such that

$$c^4a \bmod p$$

is determined to be significantly shorter than a length of the parameter b and the length of the prescribed variable p; and

determining the elliptic curve in the second form for cryptographic processing.

2. The method according to claim 1, wherein the first form of the elliptic curve is defined by $y^2 = x^3 + ax + b$.

3. The method according to claim 1, which comprises carrying out cryptographic encoding.

4. The method according to claim 1, which comprises carrying out cryptographic decoding.

5. The method according to claim 1, which comprises carrying out key allocation.

6. The method according to claim 1, which comprises carrying out a digital signature.

7. The method according to claim 6, which comprises carrying out a verification of the digital signature.

8. The method according to claim 1, which comprises carrying out an asymmetrical authentication.

9. In a device for cryptographic processing, a processor unit programmed to:

prescribe an elliptic curve in a first form, with a plurality of first parameters determining the elliptic curve;

transform the elliptic curve into a second form

$$y^2 = x^3 + c^4ax + c^6b$$

by determining a plurality of second parameters, at least one of the second parameters being shortened in length by comparison with the first parameter;

wherein x,y are variables;

a,b are the first parameters; and

c is a constant;

shorten the at least the parameter a by selecting the constant c such that

$$c^4a \bmod p$$

can be determined to be much shorter than the length of the parameter b and the length of the prescribed variable p; and

determine the elliptic curve in the second form for the purpose of cryptographic processing.

10. The device according to claim 9, wherein the device is embodied as a chip card with a memory area, the memory area being adapted to store the parameters of the elliptic curve.

11. The device according to claim 10, wherein the chip card has a protected memory area adapted to store a secret key.

12. A computer-readable medium having computer-executable instructions for performing a cryptographic processing method which comprises the steps of:

prescribing an elliptic curve in a first form, the elliptic curve having a plurality of first parameters;

transforming the elliptic curve into a second form

$$y^2 = x^3 + c^4ax + c^6b$$

by determining a plurality of second parameters, wherein at least one of the second parameters is shortened in length by comparison with the first parameter;

wherein x,y are variables;

a,b are the first parameters; and

c is a constant;

wherein at least the parameter a is shortened by selecting the constant c such that

$$c^4 a \bmod p$$

is determined to be significantly shorter than a length of the parameter b and the length of the prescribed variable p; and

determining the elliptic curve in the second form for cryptographic processing.

13. The computer-readable medium according to claim 12, wherein the first form of the elliptic curve is defined by $y^2 = x^3 + ax + b$.

Docket No.: GR 98 P 1180

COMBINED DECLARATION AND POWER OF ATTORNEY IN ORIGINAL APPLICATION

As a below named inventor, I hereby declare that: my residence, post office address and citizenship are as stated below next to my name; that I verily believe that I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

METHOD AND DEVICE FOR CRYPTOGRAPHIC PROCESSING WITH THE AID OF AN ELLIPTIC CURVE ON A COMPUTER

described and claimed in the specification bearing that title, that I understand the content of the specification, that I do not know and do not believe the same was ever known or used in the United States of America before my or our invention thereof, or patented or described in any printed publication in any country before my or our invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve month prior to this application, that I acknowledge my duty to disclose information of which I am aware which is material to the examination of this application under 37 C.F.R. 1.56a, and that no application for patent or inventor's certificate of this invention has been filed earlier than the following in any country foreign to the United States prior to this application by me or my legal representatives or assigns:

German Application No. 198 06 825.5, filed February 18, 1998, the International Priority of which is claimed under 35 U.S.C. §119; and International Application No. PCT/DE99/00278, filed February 2, 1999, the Priority of which is claimed under 35 U.S.C. §120.

I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

HERBERT L. LERNER (Reg.No.20,435)
LAURENCE A. GREENBERG (Reg.No.29,308)
WERNER H. STEMER (Reg.No.34,956)
RALPH E. LOCHER (Reg.No. 41,947)

Address all correspondence and telephone calls to:

LERNER AND GREENBERG, P.A.
POST OFFICE BOX 2480
HOLLYWOOD, FLORIDA 33022-2480
Tel: (954) 925-1100 - Fax: (954) 925-1101

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF FIRST JOINT INVENTOR: ERWIN HESS

INVENTOR'S SIGNATURE: ______________________________

DATE: ____________________

Residence: OTTOBRUNN, GERMANY

Country of Citizenship: GERMANY

Post Office Address: GOTTFRIED-KELLER-STRASSE 36
D-85521 OTTOBRUNN
GERMANY

FULL NAME OF SECOND JOINT INVENTOR: JEAN GEORGIADES

INVENTOR'S SIGNATURE: ______________________________

DATE: ____________________

Residence: MÜNCHEN, GERMANY

Country of Citizenship: GERMANY

Post Office Address: UNGERERSTRASSE 68A
D-80805 MÜNCHEN
GERMANY

Abstract of the Disclosure:

In the case of cryptographic processing with the aid of an elliptic curve, parameters of the elliptic curve are stored in a memory of a computer. These parameters are each of substantial length. The elliptic curve is transformed in order to shorten at least one parameter significantly in length and to ensure that the high security level is unchanged in the process. One parameter is preferably shortened to 1, -1, 2 or -2 with the aid of an algorithm, whereas the other parameters have a length of several 100 bits. The shortening of even one parameter is clearly reflected in the case of devices which have little memory space.

WHS:tg - 98p1180F//8/14/2000

FIG 1

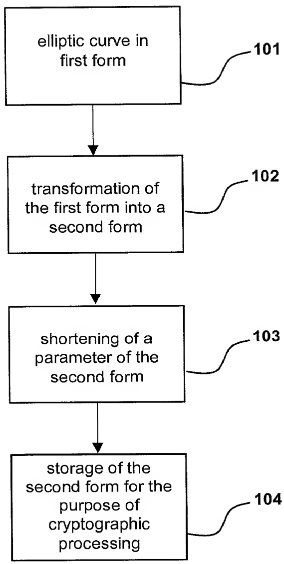

elliptic curve in first form
101
transformation of the first form into a second form
102
shortening of a parameter of the second form
103
storage of the second form for the purpose of cryptographic processing
104

FIG 2

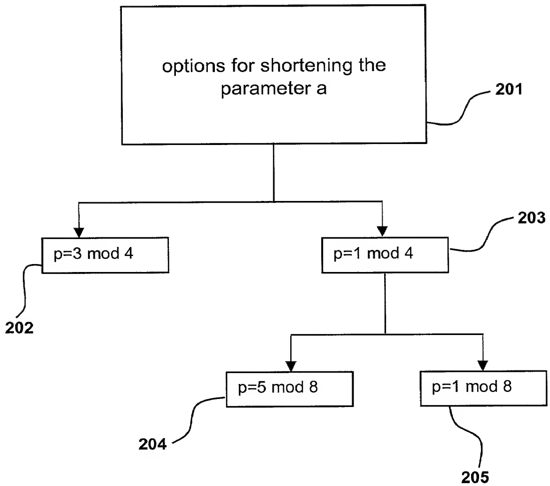

options for shortening the parameter a
201
p=3 mod 4
202
p=1 mod 4
203
p=5 mod 8
204
p=1 mod 8
205

FIG 3

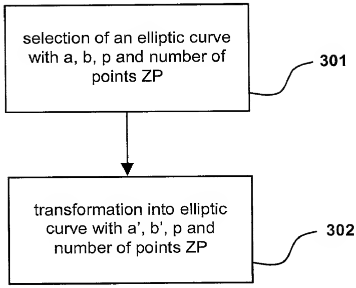
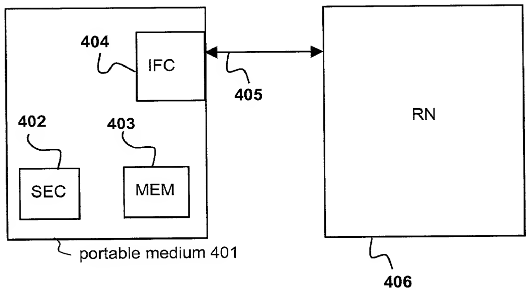

selection of an elliptic curve with a, b, p and number of points ZP
301
transformation into elliptic curve with a', b', p and number of points ZP
302

FIG 4


404
IFC
405
402
403
SEC
MEM
portable medium 401
RN
406

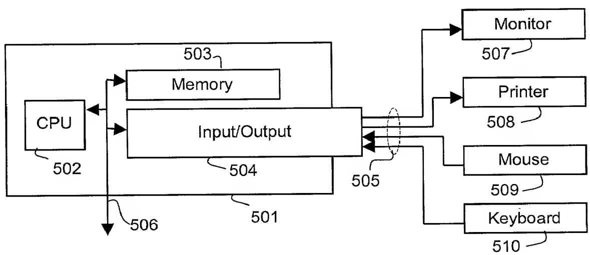

503
Memory
CPU
Input/Output
502
504
505
506
501
Monitor
507
Printer
508
Mouse
509
Keyboard
510

FIG 5